Journal of Organizational and End User Computing
Volume 33 • Issue 6 • November-December 2021

Novel Classification of IoT Devices Based on Traffic Flow Features

Ivan Cvitić, Faculty of Transport and Traffic Sciences, University of Zagreb, Croatia
https://orcid.org/0000-0003-3728-6711

Dragan Peraković, Faculty of Transport and Traffic Sciences, University of Zagreb, Croatia
https://orcid.org/0000-0002-0476-9373

Marko Periša, Faculty of Transport and Traffic Sciences, University of Zagreb, Croatia
https://orcid.org/0000-0002-0332-8648

Mirjana D. Stojanović, Faculty of Transport and Traffic Engineering, University of Belgrade, Serbia
https://orcid.org/0000-0003-1073-5804

ABSTRACT

The concept of IoT (internet of things) assumes a continuous increase in the number of devices, which raises the problem of classifying them for different purposes. Based on their semantic characteristics, meaning, functionality, or domain of usage, the system classes have been identified so far. This study's purpose is to identify device classes based on traffic flow characteristics such as the coefficient of variation of the received and sent data ratio. Such specified classes can combine devices based on behavior predictability and can serve as the basis for the creation of network management or network anomaly detection classification models. Four generic classes of IoT devices were defined using the classification of the coefficient of variation method.

KEYWORDS

Cybersecurity, Human Type Communication, Internet of Things, Machine Type Communication, Network Anomaly, Network Flow, Network Traffic, SHIoT, Smart Home

INTRODUCTION

The Internet of Things is a term defined by numerous sources of professional and scientific research literature. The idea of the IoT concept was first defined by Kevin Ashton, co-owner and CEO of Auto-ID Center in 1999. With further development and increase of application, the concept of IoT was defined by numerous professional standardization bodies, organizations and associations in the field of IK technologies, as well as numerous researchers. The IoT concept can be viewed by expanding existing human-application interaction through a new dimension of integration and communication represented by objects. The IoT concept's potential enables its implementation and application in various areas covering society, the environment, and industry.

DOI: 10.4018/JOEUC.20211101.oa12

According to the forecasts presented in Statista, (2018a), at the end of 2020, approximately 31 billion IoT devices where available globally, and until 2025 there will be 75 billion IoT devices. By doing so, 41% or 12.86 million IoT devices will be installed within the smart home (SH) concept Statista, (2018)b. Restrictions on IoT devices in general, and therefore the SHIoT (Smart Home IoT) devices are described in the research Ivan Cvitić et al. (2016), which include hardware constraints, demands for high autonomy, and low production costs, thus reducing the possibility of implementing advanced protection methods and increasing the risk of the many threats shown in Ali and Awad (2018). These device limitations in the IoT concept increase the risk of carrying out numerous cyberattacks on IoT devices or using IoT devices to pierce attacks on other targets.

Traffic generated by SHIoT devices or MTC (Machine Type Communication) traffic differs from traffic generated by conventional HTC (Human Type Communication) traffic, as shown in the survey Al-Shammari et al. (2018). Although SHIoT devices are characterized by heterogeneity, MTC traffic is homogeneous to HTC traffic, meaning that devices of the same or similar purpose behave approximately equally or generate similar traffic Laner et al., (2013). Current research focuses mainly on creating device behavioral patterns (fingerprinting) specific for an individual device or classifying them by functionality or purpose. Such an approach is not adequate nor efficient in dynamic conditions such as IoT where new devices are developed and put in the market daily with new features, functionalities, and purpose. More generic classes need to be defined in such an environment, independent of devices' semantic characteristics and based solely on network traffic features that they are generating.

This research's underlying hypothesis is that SHIoT devices can differentiate by traffic flow characteristics such as the ratio of received and sent data and that such features can be utilized to define IoT devices' classes. Such an approach is vital for the future development of cyberattack detection and mitigation systems tailored for IoT concept. This kind of classes definition will be independent of semantic categorization and functionality based classification approach, which will be applicable to IoT devices developed in the future. In that way, novel systems for traffic anomaly detection based on machine learning can be developed because it will be possible to define normal behavior profiles for each defined class of IoT device as a foundation for the detection of individual IoT device anomalous behavior.

The rest of this paper is organized as follows: subsection „Related research" deals with the current research, their shortcoming, and the positioning of our research according to previous findings. Subsection „Research methodology" explains the methodology and methods used in the research. The second section gives an overview of the smart home environment, used communication technology, and device heterogeneity. Through the same section, some of the most important cybersecurity challenges related to IoT concept are addressed. The third section represents the data collection process, including used device description, descriptive statistics of collected data, and feature extraction process explanations. In the fourth section classes of IoT devices was defined based on the coefficient of variation of device's upload and download traffic ratio. The fifth section discusses the presented approach for IoT devices class definition and feature calculations. In the final, sixth, section we gave the conclusion, final remarks, and future research direction based on this research findings.

Related Research

Identifying devices in the IoT environment is an important step. It represents the basis for activities related to the security in which such devices exist (detecting unauthorized activity, detecting unauthorized devices within the network, detecting malicious code). Meidan et al. (2017) seeks to detect unauthorized devices connected to the monitored network based on device identification. A total of 11 IoT devices have been used for this purpose, classified according to the device's semantic characteristics ie their purpose (child monitoring devices, motion sensors, refrigerators, safety cameras, smoke sensors, sockets, thermostats, televisions, clocks). A similar way of classification, based on the device's semantic characteristics, is also shown in the research by Bai et al. (2018) in which authors

use a secondary data set collected Sivanathan et al. (2017). The research covered 15 devices classified into four categories regarding each device's purpose (hubs, electronic devices, cameras, and sockets). Specific features of MTC traffic were used to address numerous problems in the communications network. Research Meidan et al. (2018) monitors the impact of MTC traffic on QoS when integrating with HTC traffic in the LTE communications network. Identification and classification of IoT devices in smart cities and campuses and smart circles using MTC traffic characteristics are shown in Sivanathan et al. (2017, 2019). Mentioned research and research (Shahid et al., 2019) seeks to use machine learning methods for identifying individual IoT devices in the network, developing and learning classification models using data generated by those IoT devices. One of the most common reasons for IoT device identification based on traffic features is to detect deviance of devices from their normal behavior. Salman et al. (2019) developed a classification model for IoT devices where every class represents an individual device. Although such a model can identify individual IoT devices and deviations in behavior, such an approach is not applicable on new and previously unseen devices. Authors Bikmukhamedov and Nadeev (2019) used machine learning methods to categorize traffic flows generated by IoT devices using traffic flow features. Such an approach differs from previous ones by not focusing only on individual devices but staying unclear how this kind of categorization can be used and for what purpose.

The current research shows that approaches to identifying and classification IoT devices are based mainly on the device's semantic features. The device classes are defined according to the mode of application of such devices or their primary functionalities Biswas et al., (2018). The lack of such an approach to defining device classes can be viewed from a smart home environment's dynamism. Therefore, the SHIoT device class needs to be defined to be applicable to upcoming SHIoT devices that will differ from the currently available devices according to their functionality and application.

This research aims to define the class of IoT devices based solely on the characteristics of traffic flows generated by such devices following the conclusions presented by I. Cvitić et al. (2019). Such defined classes will be independent of the device's semantic characteristics and functionality, which is why its application is also possible on new IoT devices that will be introduced in the future.

Research Methodology

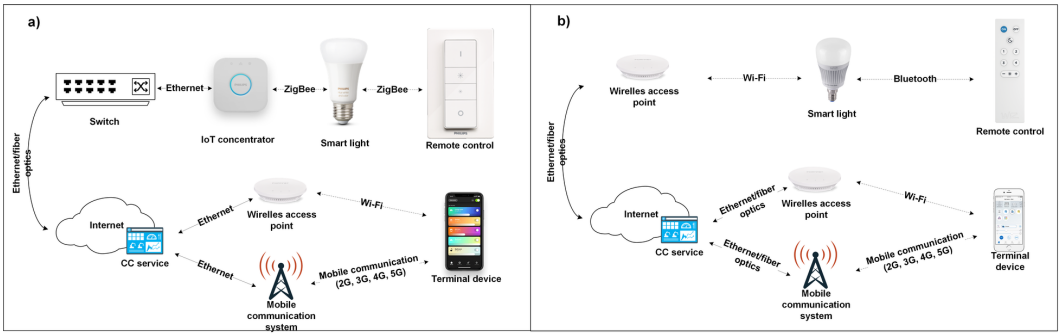
To carry out this research, primary and secondary data were collected. To collect primary data, a laboratory environment was established in the Laboratory for Security and Forensic Analysis of the Information and Communication System of the Department for Information and Communication Traffic of the Faculty of Transport and Traffic Sciences of the University of Zagreb. Secondary data used in this research were collected for research (Hamza et al., 2018; Hamza et al., 2018; Sivanathan et al., 2019). The data collected represent the traffic generated by the IoT devices covered by this research. To define the device's classes, mathematical and statistical methods and Stata software were used for data processing and interpretation of the results of the research.

SMART HOME ENVIRONMENT

The smart home is a concept of application of ubiquitous computing in the household environment. According to Alam et al. (2012), several synonyms are accepted in the scientific research and professional literature for smart home, such as home automation, intelligent home, adaptive home, and the like.

European standard EN 15232 and the Energy Performance of Buildings Directive 2010/31/EU, which is in line with Directive 2009/72/EC, as well as the Energy Plan for 2050, promote the adoption of smart home technologies to reduce energy consumption in the housing sector Lobaccaro et al. (2016). According to Bugeja et al. (2016), the smart home environment can be considered as a set of SHIoT devices, communication technologies and services. SHIoT devices are hardware units that combine sensors, actuators. Communication technologies enable the connectivity of SHIoT devices

Figure 1. Scenarios for connecting SHIoT devices in a smart home environment; a) with IoT concentrator and wired communication and b) without IoT concentrator and exclusively by wireless communication



into a single communication network, and the services provide various functionalities to end users through the use of application solutions Hamidi and Jahanshahifard (2018).

Although the emergence and rapid expansion of broadband Internet access in the late 1990s provided the technological foundation for the development of home networks, the smart home concept began to be implemented in the second half of the 2000s. The development and popularization of smartphones has contributed to this. After 2010, this concept began to develop rapidly and was based on a combination of IoT and artificial intelligence resulting in a situation-and context-aware environment (Yang et al., 2018).

A key aspect of a smart home's functioning as a backbone is developing a reliable and straightforward communication architecture. From this perspective, the smart home can be seen as a concentrator and disseminator of information and services to cover broad functional areas in the home area. The function of a smart home is not only related to communication between some aspects within the physical home in order to improve the level of comfort and quality of life but also implies performing the role of a gateway or interface to the public communications network to communicate with other concepts such as smart energy network and smart city to exchange information (Godina et al., 2015).

Communication Technologies Used in a Smart Home Environment

Devices in a smart home environment can achieve certain functionalities by local control. However, they achieve full functionalities by remote control, which requires SHIoT devices' connection to the local and public communication network Ivan Cvitić et al. (2018). The communication infrastructure used to connect SHIoT devices is also called HAN (Home Area Network). Depending on the area of operation, HAN includes LAN (Local Area Network) and PAN (Personal Area Network) or BAN (Body Area Network) communication networks and related communication technologies. Most of the communication technologies used in the HAN network were developed before the advent of the smart home environment, and most SHIoT device manufacturers use technologies such as Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), ZigBee (IEEE 802.15.4), Z-Wave or Bluetooth (IEEE 802.15.1) to achieve their network communication (Godina et al., 2015). According to Nobuyuki Hayashi, (2017), these technologies currently represent the basis of communication in the HAN network, which will continue after 2020.

The application of particular communication technology will depend on the SHIoT device's performance, purpose, and functionalities it supports. So SHIoT devices (e.g. smart thermostat) that use a battery as an energy source will also use energy-efficient communication technology (ZigBee or Z-Wave) and will communicate via IoT hubs. An IoT hub is a network device used as an intermediary in communication between two different communication technologies. This example will allow a

device using ZigBee or Z-Wave technology to communicate with a wireless access point that uses Wi-Fi technology. SHIoT devices that are connected to an uninterruptible power supply (smart sockets, smart light bulbs) will most often also use Wi-Fi communication technology.

Bluetooth technology will be used in the scenario of local connection and management of SHIoT devices. An example of such a scenario is a smart lock that detects the user's proximity using Bluetooth technology and performs the appropriate activity (e.g. unlocking the door). Due to SHIoT devices' dimensions and their potential number in the smart home environment, wireless communication technologies were primarily used due to the convenience and ease of connecting devices in the HAN network. However, individual manufacturers in specific segments of HAN infrastructure also use wired connection method (ethernet). Figure 1 shows two scenarios for connecting smart lighting fixtures. Part A of the same figure shows the IoT concentrator's application and its wired communication with the network switch, while the communication between the IoT concentrator, the lighting device, and the remote control is performed using ZigBee technology.

The purpose of an IoT hub is to connect multiple devices from the same manufacturer through the same hub. This approach aimed to create a homogeneous smart home environment where SHIoT devices from the same manufacturer would provide all functionalities. It is the result of competition and gaining a competitive advantage. However, according to Blumtritt (2019), the mentioned trend is declining, and the integration of such devices into the gateway device is expected in the future. Therefore, in the future, a more realistic connectivity scenario is shown in Figure 1b where a SHIoT device connects to a wireless access point without the need for intermediary communication devices.

Security Aspects of the Smart Home Concept Application

Various authors explore security challenges that relate predominantly to the comprehensive area of the IoT concept. According to Jing et al. (2014), the IoT concept inherits the security challenges present in sensor networks, mobile communication networks, and the Internet. However, it additionally possesses security challenges related to privacy, authentication, access control, and accessibility, which are highlighted by numerous relevant researches (Adat & Gupta, 2018; Čolaković & Hadzialic, 2018; Cvitić et al., 2016; Gupta et al., 2020; Jing et al., 2014; Pishva, 2017; Polk & Turner, 2014; Sethi & Sarangi, 2017). Cherdantseva and Hilton (2013) proves that the basic principles of security (confidentiality, integrity, and availability) or the CIA triad are not sufficient to take into account the new threats that arise as a result of the application of the IoT concept. Therefore, in addition to the CIA triad, it is proposed to consider additional principles: non-repudiation, privacy, audit, accountability, and credibility shown in Table 1.

As an area of the IoT concept application, the smart home environment provides numerous benefits to users from different aspects and through a variety of application possibilities. In parallel with the growing trend in the number of smart homes, the penetration of SHIoT devices, and the growth of investment in this concept, there is an increase in security threats. According to research by various authors, this environment consists of SHIoT devices, which have limited functionality and hardware resources. According to Ivan Cvitić et al. (2016), Bugeja et al. (2016), and Dahiya (2017), the restrictions of SHIoT devices are the result of the following requirements and characteristics:

- Size and design of the device - small dimensions of the device are often required, which results in the implementation of hardware components of even smaller dimensions and limited capabilities.
- Price of the device - due to the heterogeneity of the market and the number of manufacturers, the production of the device is required at the lowest possible price, which results in the use of components of poor quality, reliability and limited capabilities.
- Energy requirements - devices must meet high requirements in terms of autonomy while implementing energy-efficient components.
- Heterogeneity - a large number of devices that use different communication technologies and proprietary protocols.

Table 1. Extended security principles necessary in environments applying the IoT concept

The principle of security	Explanation	Resources of the IC system to which the principle applies					
		Data	Users	Processes	Hardware	Software	Network
Confidentiality	Only authorized users/processes have the right to inspect and access the resources of the IC system		●				
Integrity	Only authorized users have the right to change the data in the IC system			●			
Availability	IC resources must be available to the legitimate user/process at the required time and according to the given conditions	●	●	●	●	●	●
Non-repudiation	Participants in a transaction that takes place through the IC system cannot deny the execution of the transaction	●	●	●	●	●	●
Privacy	The ability of the IC system to enforce defined privacy rules allowing the user to control sensitive data	●					
Audit	The ability of the IC system to enable the implementation of an audit of activities in case of adverse event	●	●	●	●	●	●
Accountability	The ability of the IC system to impose responsibility on the user for the actions taken	●		●			
Credibility	The ability of the IC system to unambiguously establish identity and ensure trust between third parties (users/processes)	●	●				

Source: Cherdantseva & Hilton (2013)

Limited hardware resources in SHIoT devices that result from these requirements prevent the implementation of adequate protection methods such as advanced cryptographic algorithms. In doing so, SHIoT devices remain exposed to many threats that have the potential to violate the basic principles of security (confidentiality, integrity, and availability) of such devices. Today's facilities are not built and designed as smart homes, but SHIoT devices are retrogradely implemented in the existing environment and contribute to security challenges. Also, there is no professional support when designing a smart home or operating a SHIoT device in a home environment Lin and Bergmann (2016). An additional factor that affects the low level of security of SHIoT devices is their adaptability to end-users. To make SHIoT devices available to as many users as possible, manufacturers had to simplify their configuration to require minimal user interaction, such as connecting devices to an access point using WPS (Wi-Fi Protected Setup) whose vulnerabilities are known and proven Sanatinia et al., (2013). This results in SHIoT devices that do not have basic security mechanisms such as encrypted communication when connecting and configuring devices or device access data (username and password) (Geneiatakis et al., 2017).

SHIoT devices collect, process, store and transmit data of different levels of sensitivity. In the case of unauthorized access, such data may be used for various purposes such as identity theft, unauthorized access to users' private data and monitoring of user behavior (Desai & Upadhyay, 2014). In addition to the above, there is a possibility of partial or complete disabling of the SHIoT device, which loses a smart home's functionality. Improper functioning of SHIoT devices can also lead to disruption of the physics of human or object safety due to the increasing reliance of users on the information provided by such devices (Apthorpe et al., 2017). An example of this is the malfunction of a fire detector that alerts emergency services. Finally, SHIoT devices can also be used as intermediaries or a means to carry out other forms of attacks (DDoS – Distributed Deanial of Service attacks; Bugeja et al., 2016; Ivan Cvitić, 2020; Ivan Cvitić et al., 2019; Stergiou et al., 2018).

DATA COLLECTION AND PROCESSING

The SHIoT devices covered by this research are presented in Table 2. The MAC (Media Access Control) represents unique identifiers of the SHIoT device in the network, the name of the device, the P / S tag that indicates whether the monitored device used for collecting primary or secondary data, and to which group belongs according to the segmentation shown in Ivan Cvitić et al. (2018).

SHIoT devices are provided by authorized distributors and dealers of a single device manufacturer. They are connected to and connected to the communications network in ways recommended by the manufacturer and in no way have the devices modified at the software and hardware level. Therefore, it is assumed that the devices used to collect legitimate traffic within this research work in the way they are designed and in no way compromised in any way.

The network topology and the characteristics of a smart home environment can be seen in Figure 2. Devices are connected directly or indirectly with Wi-Fi communications technology with the Fortinet AP 221C wireless access point, except for the Phillips Hue device that communicates with the rest of the local network via Ethernet communication technology. Some devices, such as the Blink Smart Camera, the Netatmo Smart Thermostat and the Philips Hue Smart Bulb, use IoT hubs with wireless communication and ZigBee technology. This is the energy efficiency of the device as it uses the battery as the ultimate power source, which gives them advantages from the aspect of mobility and independence of the power supply unit as a source of power. The IoT hub is connected to Wi-Fi (or Ethernet in the case of a Phillips Hue device) with a wireless access point technology. The subject mentioned as an adequate point of collecting traffic that SHIoT devices generate is a certain wireless access point. Because of computers and wireless Wi-Fi networks' known working methods and characteristics, communication in the communications network cannot be collected directly. Several methods are available for collecting traffic, but mirroring the switch's physical port is often used. The mentioned method proved to be effective in several studies such as Amar et al. (2018), Karimi et al. (2016), Meidan et al. (2017, 2018), which provides the basis for applying the same method for this research.

To collect network traffic, the port mirroring functionality is set up with a software-hardware platform consisting of a wireless access point, the Fortinet AP 221C, the Cisco 2960 Catalyst 48 PoE (Power over Ethernet) switch, and the HP Pavilion dm1 workstation (Microsoft Windows 10 10.0. 17134 build 17134, x64 processor architecture, AMD E-350, 1600MHz 2 core, 4 GB RAM) with installed Wireshark software tool version 2.6.3.

Extraction of Traffic Flows of IoT Devices

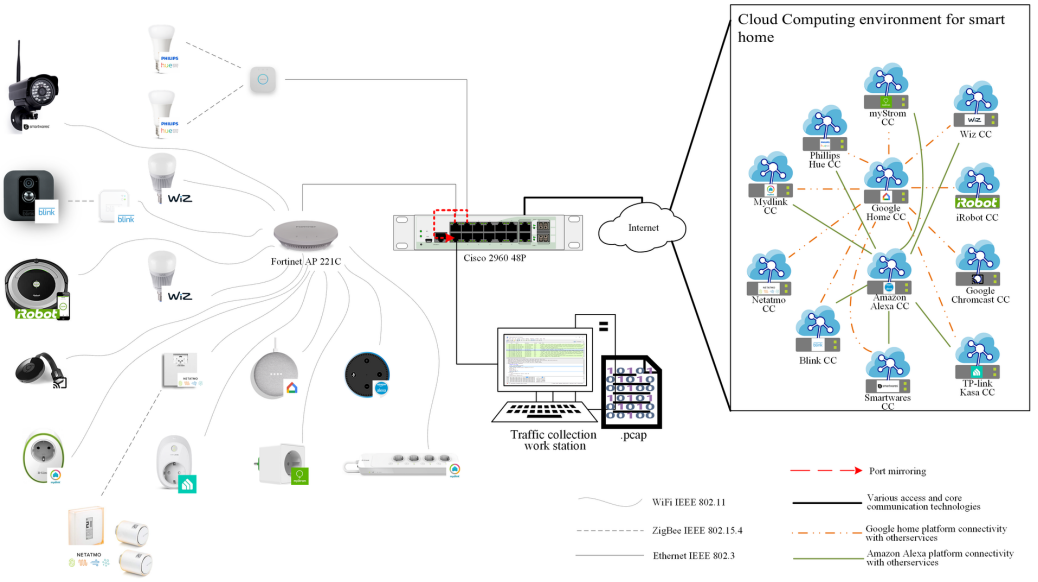
Defining the class of SHIoT devices in this research is based on the statistical characteristics of a particular device's traffic flows. The traffic flow is defined by a packet with equal source of source IP address, destination IP address, source communication port, destination communication port, and protocol used (TCP or UDP) (Aghaei-Foroushani & Zincir-Heywood, 2015). The reason for choosing a traffic flow as the level of observation and analysis of the feature is that it represents the packet header's aggregated (statistical) data for communication between the source and the destination. The packet-level traffic analysis includes more information such as packet content and more computing resources for their storage and processing. An example of the number of traffic flows and the number of packets over a 24-hour time is visible to the Google Chromecast device (covered by this survey), where 11877 individual traffic flows were generated while the number of packets collected in the same time interval was 2459538. Since most today's devices and applications use cryptographic methods in the communication process, the package's content cannot be observed and analyzed economically, time-consuming, and legally acceptable. Consequently, observation and analysis of traffic characteristics at the traffic flow level are acceptable and frequently used in many researches. Extraction of traffic flow features for individual SHIoT device was done using the software tool developed at CICFlowMeter Canadian Institute for Cyber Security at the University

Table 2. SHIoT devices for data collection

No.	MAC address	SHIoT device name	Data aggregation source	Functional category
1	00:17:88:78:0a:cb	Phillips Hue Starter kit 2xE26	P	CL
2	00:17:88:2b:9a:25	Phillip Hue Starter kit 4xE26	S	CL
3	a8:bb:50:05:31:f3	WiZ Colors ESP_0531F3	P	CL
4	a8:bb:50:05:06:b0	WiZ Colors ESP_0506B0	P	CL
5	d0:73:d5:01:83:08	Light Bulbs LiFX Smart Bulb	S	CL
6	00:24:e4:20:28:c6	Withings Aura Sleep Tracking Mat	S	CL
7	7c:2e:bd:3d:4f:cb	Google Chromcast	P	M
8	18:b7:9e:02:20:44	Invoxia Triby Speaker	S	M
9	e0:76:d0:33:bb:85	PIX-STAR Photo-frame	S	M
10	fc:65:de:31:69:d6	Amazon Alexa Dot	P	M
11	44:65:0d:56:cc:d3	Amazon Alexa Echo	S	M
12	20:df:b9:21:fd:79	Google Home mini	P	M
13	ac:84:c6:5d:97:bc	TPlink Smart Plug HS110	P	MC
14	50:c7:bf:00:56:39	TPlink Smart Plug HS105	S	MC
15	30:ae:a4:57:2d:54	MyStrom switch	P	MC
16	74:da:da:5f:a8:19	D-link DSP-W245 plug	P	MC
17	74:c6:3b:29:d7:1d	iHome Power Plug	S	MC
18	ec:1a:59:79:f4:89	Belkin Wemo switch	S	MC
19	d0:52:a8:00:67:5e	Samsung Smart Things	S	MC
20	74:6a:89:00:2e:25	Blipcare Blood Pressure meter	S	MC
21	70:88:6b:10:0f:c6	Awair air quality monitor	S	MC
22	40:9f:38:e9:28:08	iRoobot Roomba 896	P	SA
23	80:c5:f2:bb:17:95	iRoobot Roomba 895	P	SA
24	00:24:e4:1b:6f:96	Withings Body	S	SA
25	e8:ab:fa:9b:f0:9e	Smartwares C923IP Camera	P	S
26	00:03:7f:27:2c:c3	Blink XT2 Camera	P	S
27	7c:70:bc:5d:5e:dc	Canary View Camera	S	S
28	70:ee:50:18:34:43	Netatmo Welcome Camera	S	S
29	f4:f2:6d:93:51:f1	TPlink Day Night Cloud NC220 camera	S	S
30	00:16:6c:ab:6b:88	Samsung SmartCam	S	S
31	30:8c:fb:2f:e4:b2	Nest Dropcam	S	S
32	00:24:e4:11:18:a8	Withings Smart Baby Monitor	S	S
33	18:b4:30:25:be:e4	NEST Protect Smoke Alarm	S	S
34	88:4a:ea:31:66:9d	Ring Video Doorbell	S	S
35	70:ee:50:0c:14:c2	Netatmo Smart Thermostat	P	EM
36	70:ee:50:03:b8:ac	Netatmo Smart Weather Station	S	EM

*P – Primary; S – Secondary; CL – Comfort and Lightning; M – Multimedia; MC – Monitor and Connectivity; S – Security; SA – Smart Appliances; EM – Energy Management

Figure 2. Smart home laboratory environment



of New Brunswick in Canada (Habibi Lashkari et al., 2017). This tool allows the extraction of 84 traffic flow characteristics such as source and destination IP addresses, time of the traffic flow, interarrival time of packets, packet number per traffic flow, packet size, amount of data transferred, transfer rate, and so on.

The period for which the feature extraction is performed is 30 consecutive days, with a different number of generated traffic flows depending on the device and its characteristics.

DEFINING SHIOT DEVICE CLASSES

Classes of SHIoT devices are defined based on traffic flow features. For this purpose, the coefficient of variation of the ratio of the received and sent volume of traffic is used, which represents the index of the predictability level of the IoT's behavior.

Determination of Features for Defining SHIoT Device Classes

The predictability of the IoT devices behavior is a phenomenon resulting from the communication activities of IoT devices observed in the research (Amar et al., 2018; Doshi et al., 2018; Meidan et al., 2018). Since IoT devices have a limited number of functionalities, certain devices will behave approximately the same over time according to the values of the observed traffic features. Unlike IoT devices, conventional devices (smartphones, desktops, laptops, etc.) support installing a large number of applications where the communication activity of such devices depends on end-users and how the device is used. According to the above, the IoT device predictability level indices expressed by the coefficient of variation of received and sent data (C_u index) is a measure based on which it is possible to determine the IoT device's behavior over a given period of time. As the C_u index is closer to 0, the observed device has less deviation of the amount of received and sent data, and the level of predictability of such device behavior is considered to be greater than the device whose C_u index is greater than 0.

The C_u index is calculated for mean values of 20 consecutive traffic flows of a single SHIoT device over a time period of 30 days according to expression (1).

$$C_u = \frac{\sqrt{\frac{1}{N-1}\sum_{i=1}^{N}\left(x_i - \overline{x}\right)^2}}{\frac{1}{N}\sum_{i=1}^{N} x_i} \quad (1)$$

Where:

C_u – index of traffic predictability level for SHIoT device *u*

N – total number of mean values of the received and sent data volume ratio for 20 consecutive traffic flows in the time period t = 30 days

x_i –the mean value of received and sent data volume ratio for 20 consecutive traffic flows

In order to avoid that the mean values to tend 0, which is the problem of the coefficient of variation method application as a normalized dispersion value in the data set, the traffic flows in which the ratio of received and sent data is equal to 0 is removed.

Defining the IoT Device Classes Based on the Coefficient of Variation

For the purpose of the SHIoT device classes definition based on the C_u index value, the coefficient of variation classification method applied by Couto et al. (2017), Ferreira et al. (2019), Romano et al. (2005), Vaz et al. (2017) was used. It assumes normal data distribution. Since the distribution of the obtained values (C_u index) are asymmetric in nature (negative skewness) the data have been transformed. The data transformation method was selected using the Ladder of powers (Tukey method) to clearly show a suitable data transformation function to achieve normal distribution (Ernst et al., 2017). Table 3 shows the chi2 values of a particular transformation function. The data distribution is closest to the normal chi^2 closer to 0 and P (chi^2) closer to 1. The normal distribution of the data obtained is also confirmed by the Shapiro-Wilk test of normality (p = 0.7262).

To apply the method of classifying the coefficient of C_u index, it is normalized by the min-max method according to the expression (2):

$$C_{u(norm)} = \frac{\log\left(C_u\right) - \log(C_{umin})}{\log(C_{umax}) - \log\left(C_{umin}\right)} \quad (2)$$

Where:

$C_{u(norm)}$ – the normalized value of the logarithmically transformed C_u index in the interval [0,1]

$\log\left(C_u\right)$ – logarithmic value of C_u device *u*

$\log(C_{umin})$ – minimum logarithmic value of C_u for all devices

$\log(C_{umax})$ – maximum logarithmic value C_u for all devices

After the normal distribution of the data was established, classifying the coefficient of variation is applied. It is a result of the mean coefficient variation values and their standard deviations.

The mean value of the coefficient of variation is calculated according to (3):

$$A_{C_{u(norm)}} = \frac{1}{N}\sum_{u=1}^{n}\frac{C_{1(norm)} + C_{2(norm)} + \cdots + C_{n(norm)}}{N} \quad (3)$$

Where:

Table 3. Ladder of powers results

Transformation	Formula	chi2	P(chi2)
Cubic	C_u^3	50,29	0
Square	C_u^2	42,42	0
Identity	C_u	25,18	0
Square root	$\sqrt{C_u}$	12,08	0,002
Logarithmic	**log(C_u)**	**0,44**	**0,804**
1/(square root)	$\sqrt{\frac{1}{C_u}}$	9,48	0,009
Inverse	$\frac{1}{C_u}$	25,07	0
1/square	$\frac{1}{C_u^2}$	43,37	0
1/cubic	$\frac{1}{C_u^3}$	51,08	0

$A_{C_{u(norm)}}$ – the arithmetic mean of the coefficient of variation for all devices
N – number of SHIoT devices
$C_{u(norm)}$ – coefficient of variation of the device u
The standard deviation of the coefficient of variation was calculated according to the formula (4):

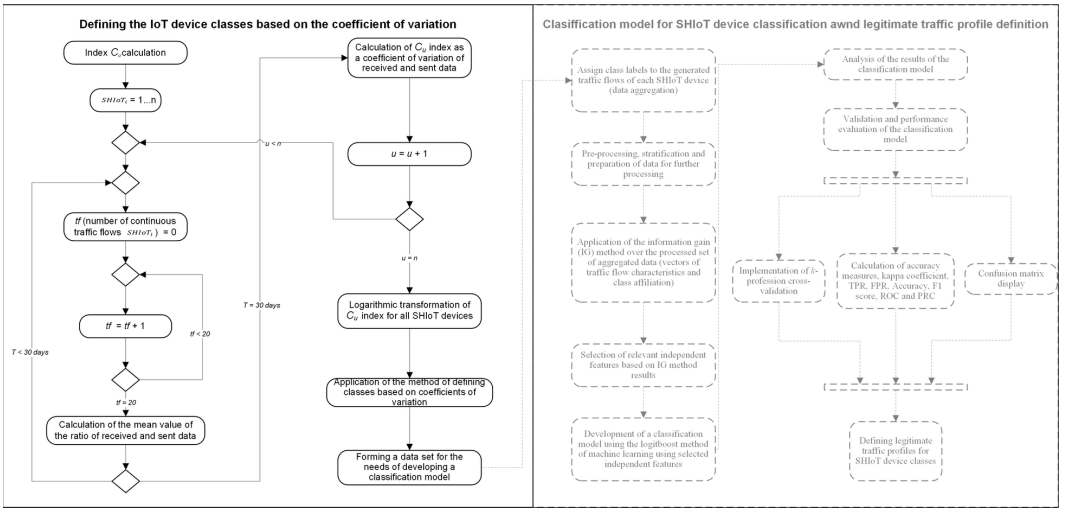
$$\sigma_{C_{u(norm)}} = \sqrt{\frac{1}{N-1}\sum_{u=1}^{n}(C_{u(norm)} - \bar{C})^2} \quad (4)$$

Where:

$\sigma_{C_{u(norm)}}$ – standard deviation of the coefficient of variation for all devices
N – number of SHIoT devices
$C_{u(norm)}$ – coefficient of variation of the device u
$\bar{C}$ – the arithmetic mean of the coefficient of variation for all devices

Based on previously performed data processing, a total of 4 classes of IoT devices were defined according to the method used in the research Romano et al., (2005). The first class includes devices for which the condition is met $C_{u(norm)} \leq A_{C_{u(norm)}} - \sigma_{C_{u(norm)}}$. The second class includes devices that

Figure 3. Current and future research process and activities



meet the condition $A_{C_{u(norm)}} - \sigma_{C_{u(norm)}} < C_{u(norm)} \leq \frac{A_{C_u} + \sigma_{C_u}}{2}$. The third class includes devices that meet the condition $\frac{A_{C_u} + \sigma_{C_u}}{2} < C_{u(norm)} \leq A_{C_u} + \sigma_{C_u}$, while the last class includes devices that meet the condition $C_{u(norm)} > A_{C_u} + \sigma_{C_u}$.

RESEARCH RESULTS AND DISCUSSION

For this research, the classification of coefficient of variation method was used to define the clasess of IoT devices based on the ratio of received and sent data in the given time. This method was previously used in different research fields but through its analysis we concluded that it is suitable for solving the problem represented in this research, and that is how to distinguish various IoT devices based on their network traffic behavior. For this purpose we define index C_u as the ratio of sent and received data for individual IoT device. By using the classification of the coefficient of variation method we managed to define a level of IoT device behavior predictability and get the solid stronghold for future research of IoT devices classification. Values of C_u index, logarithmically transformed values, and min-max normalized values for each analyzed device are shown in Table 4.

Figure 3 shows phases of conducted research through UML activity diagram (on the left) and future planned research (on the right). It is visualized, for better understanding, all main activities conducted for defining classes of SHIoT devices covered by this research. For every device (*d*), traffic flows (*tf*) are extracted in 30 consecutive days, where we observed the amount of sent and received data and calculate its mean value. It was the basis for calculating index C_u as the sent and received ratio of the variation coefficient. Given values for every SHIoT device are logarithmically transformed for the data to follow a normal distribution as a requirement for applying the method of variation coefficient classification.

According to the data presented in Table 4, four device classes are defined based on the C_u index value. The first class (C1) comprises all devices whose log-transformed and normalized value $C_{u(norm)}$ £ 0,253722. The second class (C2) combines devices that meet the requirement 0,253722 < $C_{u(norm)}$

Table 4. Device classes defined by the value of index C_u

No.	SHIoT device	Index C_u	log(C_u) transformation	Min-max normalization ($C_{u(norm)}$)	Class definition	Class name
1	TPlink Day Night Cloud NC220 camera	0,042916917	-1,367371486	0	$C_{u(norm)} \leq A_{C_u} - \sigma_{C_u}$	C1
2	WiZ Colors ESP_0531F3	0,075820416	-1,120213838	0,124242056		
3	TPlink Smart Plug HS105	0,076231674	-1,117864541	0,125423008		
4	WiZ Colors ESP_0506B0	0,08086321	-1,092249024	0,138299504		
5	Samsung Smart Things	0,123562483	-0,908113372	0,230861447		
6	iHome Power Plug	0,148887517	-0,827141714	0,271564558	$A_{C_u} - \sigma_{C_u} < C_{u(norm)} \leq \frac{A_{C_u} + \sigma_{C_u}}{2}$	C2
7	Withings Smart Baby Monitor	0,176239975	-0,753895577	0,308384178		
8	NEST Protect Smoke Alarm	0,192606687	-0,715328639	0,327771139		
9	Phillips Hue Starter kit 2xE26	0,200187894	-0,69856219	0,336199355		
10	Canary View Camera	0,209863653	-0,678062771	0,346504073		
11	Tplink Hs110	0,24742122	-0,606563056	0,382445795	$\frac{A_{C_u} + \sigma_{C_u}}{2} < C_{u(norm)} \leq A_{C_u} + \sigma_{C_u}$	C3
12	Belkin Wemo Switch	0,254614637	-0,594116633	0,388702406		
13	Witthings Sleep	0,261184872	-0,583051981	0,394264423		
14	D-link DSP-W245 plug	0,27041724	-0,567965624	0,401848085		
15	Netatmo Smart Thermostat	0,290797956	-0,53640865	0,417711253		
16	Amazon Alexa Dot	0,318918293	-0,496320569	0,437862868		
17	Blink XT2 Camera	0,344500361	-0,462810319	0,454707915		
18	Samsung SmartCam	0,34686605	-0,459838205	0,456201948		
19	Light Bulbs LiFX Smart Bulb	0,346886878	-0,459812128	0,456215056		
20	Smartwares C923IP Camera	0,357559305	-0,446651916	0,462830477		
21	iRoobot Roomba 895	0,358681004	-0,445291624	0,463514273		
22	iRoobot Roomba 896	0,379012744	-0,421346187	0,475551248		
23	MyStrom switch	0,432393144	-0,364121201	0,5043173		
24	Blipcare Blood Pressure meter	0,479127026	-0,319549331	0,526722841		
25	Netatmo Smart Weather Station	0,543491131	-0,264807539	0,554240633		
26	Amazon Alexa Echo	0,632948837	-0,198631394	0,587506285		
27	Netatmo Welcome Camera	0,764635407	-0,116545595	0,628769456		
28	Phillip Hue Starter kit 4xE26	0,791347539	-0,101632744	0,636265899		
29	PIX-STAR Photo-frame	0,958787396	-0,018277684	0,678167108		
30	Withings Body	1,140461786	0,057080738	0,716048538	$C_{u(norm)} > A_{C_u} + \sigma_{C_u}$	C4
31	Google Chromcast	1,267801595	0,103051294	0,739157175		
32	Ring Video Doorbell	1,370122066	0,136759261	0,756101612		
33	Nest Dropcam	1,985562839	0,297883636	0,837096166		
34	Invoxia Triby Speaker	2,468462951	0,392426613	0,884621355		
35	Awair air quality monitor	2,553917945	0,40720694	0,89205118		
36	Google Home mini	4,187473486	0,62195207	1		

0,354866. The third class (C3) includes devices that meet the requirements $0{,}354866 < C_{u(norm)} \leq 0{,}709732$ while the last class (C4) includes devices that meet the requirements $C_{u(norm)} > 0{,}709732$.

Class C1 signifies IoT devices with a very high level of behavior predictability since the coefficient of variation in the received and sent data ratio is closest to 0. This means that such devices over time behave approximately the same from the aspect of the observed feature. The use of IoT devices of class C1 devices by users, other devices or the environment will not significantly affect the change in the value of the C_u index. Class C2 combines devices with a high level of behavior predictability. The use of devices from the specified class by users, other devices or the environment may result in minor changes in the relationship between received and sent data. Devices classed with C3 represent devices with a medium level of behavior predictability. The impact of interaction between users, other devices or the environment on the relationship between received and sent data can be significant. Such behavior may be the additional functionalities of devices that at certain times result in a greater amount of data in the incoming or outgoing direction. The last class C4, combines IoT devices with low levels of behavior predictability. Such devices and their interaction with the user, other devices, or environment significantly affect the relationship between received and sent data. As a reason, a significantly higher amount of data is received in the incoming direction (download) due to the user's request. An example is visible to devices such as Google Chromecast where a user plays video content that requires downloading the same through a Youtube service. This class also includes the Google Home mini device, a smart speaker that can provide different audio content on a user's request, which also causes a greater variation in the relationship between received and sent traffic.

With respect to classes based on semantic features, this way of class definition allows comprising of IoT devices that are not covered by this research based on their behavior that the C_u index can measure. Given the accelerated development and the increasingly frequent application of the IoT concept, classes defined by this research will be able to consolidate IoT devices regardless of their functionalities, purpose and capabilities.

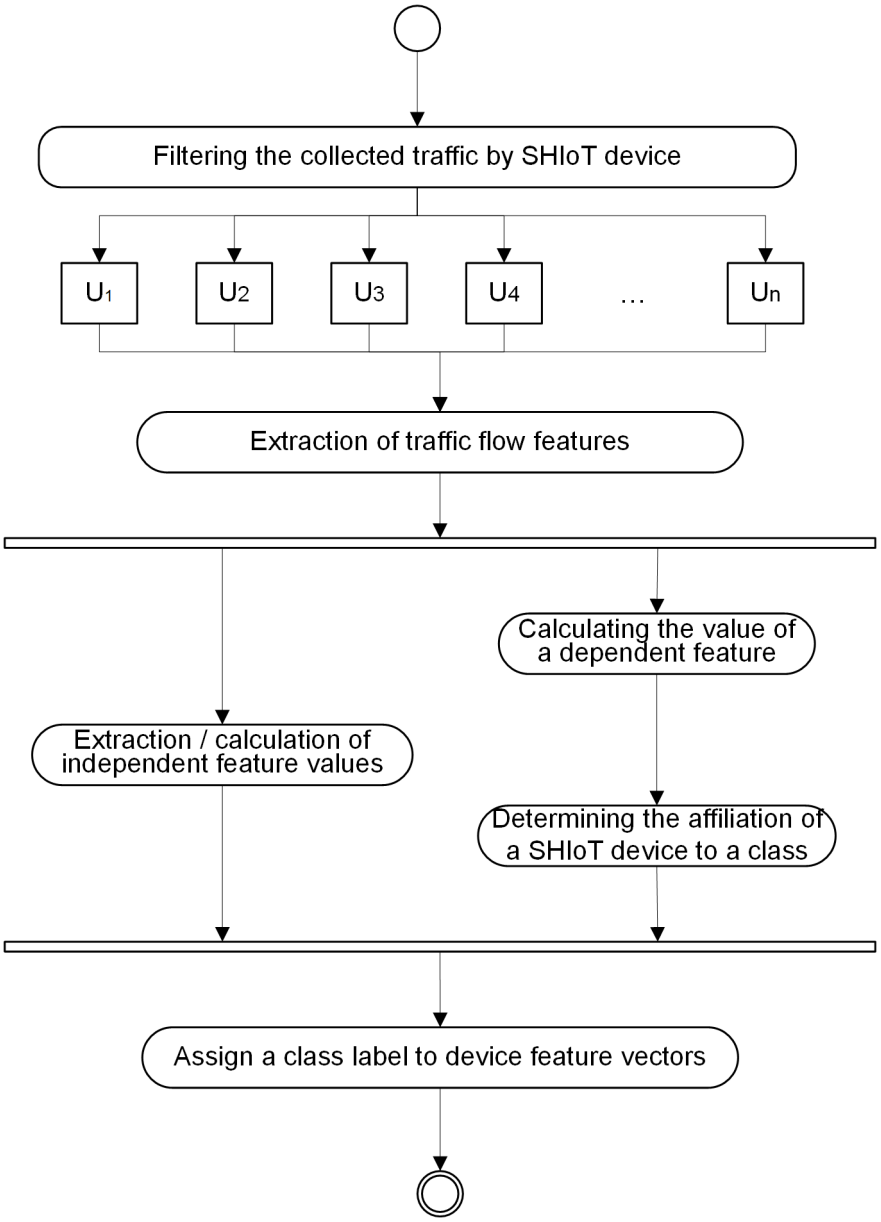
Feature vectors (examples) of traffic flow are labeled according to previously acquired findings and defined classes. The process of forming a dataset containing aggregated data of feature values for traffic flows and the traffic flow affiliation to the defined classes is shown by the UML activity diagram in Figure 4. Each traffic flow is generated by a SHIoT device belonging to a particular class according to the classification shown in Table 4. Therefore, it is associated with every traffic flow, the corresponding class to which the device generating the observed traffic flow belongs, as it is shown in Table 5.

Extraction of traffic flow feature generated by the individual SHIoT device described through this paper and defining their classes represents foundations for creating dataset containing class labels for each observed traffic flow. Such formed dataset can be used for further development of novel classification and anomaly detection models.

CONCLUSION

The classification of devices in the IoT concept is a challenging research problem. As an initial problem arises way in which it is possible to define and distinguish IoT devices. Previous research defines the classes based on the device's semantic characteristics and their purpose and scope of application. Such a class definition method represents a potential problem for new devices whose application and characteristics will differ from the existing ones. To solve this problem, this research has defined classes based on traffic features. The coefficient of variation of the received and sent dana ratio for an individual device (index Cu) was used to define the class. The C_u index was calculated for a total of 36 SHIoTs based on an average of 20 consecutive traffic flows over a 30-day time period and represents the scattering measure of the received and sent data. The data were analyzed, transformed, and normalized using the Stata tool for statistical analysis and using logarithmic transformation and min-max normalization method. The variation coefficient classification method was applied

Figure 4. Process of aggregated dataset formation



to define four classes of devices according to the predictability level of their behavior (C1 - very high level; C2 - high level; C3 - middle level; C4 - low level). The class of IoT devices defined in this way provides a framework for further research in the area of classification of the IoT device to identify their behavior and detect anomalies of network traffic that such devices can generate. Further research will seek to develop a classification model that will, on the basis of the value of the traffic flow characteristics of a variety of IoT devices, be assigned to the classes defined by this research. Such a developed classification model will be the basis for further research of various cybersecurity problems that are coming with the concept of IoT, mainly in the domain of detection, mitigation, and protection of DDoS attacks or other cyber attacks that can be identified by network traffic analysis.

Table 5. Example of combining traffic flows and class designations

No.	Device	z8	z9	z10	z11	z12	z13	z14	z15	…	z83	Class label
1	u6	110,176,901	5	4	372	648	186	0	74	…	54,900,000	C1
2	u6	110,117,149	5	4	372	648	186	0	74	…	54,800,000	C1
3	u4	113,285,202	30	23	2,012	3,831	267	0	67	…	5,740,188	C1
4	u11	9,383	7	1	2,156	308	308	308	308	…	0	C2
5	u11	1,649	3	1	924	308	308	308	308	…	0	C2
6	u10	4,785,250	17	1	5,104	296	305	296	300	…	0	C2
7	u30	104,123,962	2	4	96	192	48	48	48	…	49,300,000	C3
8	u30	2,090	1	3	33	143	33	33	33	…	0	C3
9	u30	2,126	1	3	33	143	33	33	33	…	0	C3
10	u41	141,088	4	7	454	2,881	357	28	114	…	0	C4
11	u42	68,231	1	3	32	140	32	32	32	…	0	C4
12	u43	15,158,091	9	9	6,181	3,268	1,350	23	687	…	14,900	C4

REFERENCES

Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: Issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, *67*(3), 423–441. doi:10.1007/s11235-017-0345-9

Aghaei-Foroushani, V., & Zincir-Heywood, A. N. (2015). A Proxy Identifier Based on Patterns in Traffic Flows. *2015 IEEE 16th International Symposium on High Assurance Systems Engineering*, 118–125. doi:10.1109/HASE.2015.26

Al-Shammari, B. K. J., Al-Aboody, N., & Al-Raweshidy, H. S. (2018). IoT Traffic Management and Integration in the QoS Supported Network. *IEEE Internet of Things Journal*, *5*(1), 352–370. doi:10.1109/JIOT.2017.2785219

Alam, M. R., Reaz, M. B. I., & Ali, M. A. M. (2012). A review of smart homes - Past, present, and future. *IEEE Transactions on Systems, Man and Cybernetics. Part C, Applications and Reviews*, *42*(6), 1190–1203. doi:10.1109/TSMCC.2012.2189204

Ali, B., & Awad, A. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors (Basel)*, *18*(3), 817. doi:10.3390/s18030817 PMID:29518023

Amar, Y., Haddadi, H., Mortier, R., Brown, A., Colley, J., & Crabtree, A. (2018). *An Analysis of Home IoT Network Traffic and Behaviour*. https://arxiv.org/abs/1803.05368

Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., & Feamster, N. (2017). *Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic*. 10.1109/TNSM.2009.090604

Bai, L., Yao, L., Kanhere, S. S., Wang, X., & Yang, Z. (2018). Automatic Device Classification from Network Traffic Streams of Internet of Things. *2018 IEEE 43rd Conference on Local Computer Networks (LCN),* 1–9. doi:10.1109/LCN.2018.8638232

Bikmukhamedov, R. F., & Nadeev, A. F. (2019). Lightweight Machine Learning Classifiers of IoT Traffic Flows. *2019 Systems of Signal Synchronization Generating and Processing in Telecommunications*, 1–5. Advance online publication. doi:10.1109/SYNCHROINFO.2019.8814156

Biswas, S., Devi, D., & Chakraborty, M. (2018). A hybrid case based reasoning model for classification in internet of things (IoT) environment. *Journal of Organizational and End User Computing*, *30*(4), 104–122. doi:10.4018/JOEUC.2018100107

Blumtritt, C. (2019, Dec.). Smart Home Report 2019. *Control and Connectivity*.

Bugeja, J., Jacobsson, A., & Davidsson, P. (2016). On Privacy and Security Challenges in Smart Connected Homes. *2016 European Intelligence and Security Informatics Conference*, 172–175. doi:10.1109/EISIC.2016.044

Cherdantseva, Y., & Hilton, J. (2013). A Reference Model of Information Assurance. *2013 International Conference on Availability, Reliability and Security*, 546–555. doi:10.1109/ARES.2013.72

Čolaković, A., & Hadzialic, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. *Computer Networks*, *144*, 17–39. doi:10.1016/j.comnet.2018.07.017

Couto, M. F., Peternelli, L. A., & Barbosa, M. H. P. (2017). Classification of the coefficients of variation for sugarcane crops. *Ciência Rural*, *43*(6), 957–961. doi:10.1590/S0103-84782013000600003

Cvitić, I., Vujić, M., & Husnjak, S. (2016). Classification of Security Risks in the IoT Environment. *26th Daaam International Symposium on Intelligent Manufacturing and Automation*, 731–740. doi:10.2507/26th.daaam.proceedings.102

Cvitić, I., Peraković, D., Periša, M., & Botica, M. (2018). Smart Home IoT Traffic Characteristics as a Basis for DDoS Traffic Detection. *Proceedings of the 3rd EAI International Conference on Management of Manufacturing Systems*, 1–10. doi:10.4108/eai.6-11-2018.2279336

Cvitić, I., Peraković, D., Periša, M., & Husnjak, S. (2019). An Overview of Distributed Denial of Service Traffic Detection Approaches. *PROMET – Traffic & Transportation, 31*(4), 453–464. 10.7307/ptt.v31i4.3082

Cvitić, I. (2020). *Network Traffic Anomaly Detection Based on Traffic Characteristics and Device Class Affiliation* (Doctoral dissertation). University of Zagreb.

Cvitić, I., Peraković, D., Periša, M., & Botica, M. (2019). Novel approach for detection of IoT generated DDoS traffic. *Wireless Networks*. Advance online publication. doi:10.1007/s11276-019-02043-1

Dahiya, M. (2017, Dec.). Issues and Countermeasures for Smart Home Security Research. *Engineering Issues and Countermeasures for Smart Home Security*.

Desai, D., & Upadhyay, H. (2014). Security and Privacy Consideration for Internet of Things in Smart Home Environments. *International Journal of Engineering Research and Development*, *10*(11), 73–83. http://www.ijerd.com/paper/vol10-issue11/Version_1/J10117383.pdf

Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine Learning DDoS Detection for Consumer Internet of Things Devices. *2018 IEEE Security and Privacy Workshops (SPW)*, 29–35. 10.1109/SPW.2018.00013

Ernst, P. A., Thompson, J. R., & Miao, Y. (2017). Tukey's transformational ladder for portfolio management. *Financial Markets and Portfolio Management*, *31*(3), 317–355. doi:10.1007/s11408-017-0292-1

Ferreira, A. A. S. N. de C., Dourado, L. R. B., Biagiotti, D., Santos, N. P. da S., Nascimento, D. C. N., & Sousa, K. R. S. (2019). Methods for classifying coefficients of variation in experimentation with poultrys. *Comunicata Scientiae*, *9*(4), 565–574. doi:10.14295/cs.v9i4.2619

Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017). Security and privacy issues for an IoT based smart home. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings*, 1292–1297. doi:10.23919/MIPRO.2017.7973622

Godina, R., Rodrigues, E., Matias, J., Catalão, J., & Mendes, T. (2015). Smart Home Communication Technologies and Applications: Wireless Protocol Assessment for Home Area Network Resources. Energies, 8(7). doi:10.3390/en8077279

Gupta, B. B., Chaudhary, P., & Gupta, S. (2020). Designing a XSS Defensive Framework for Web Servers Deployed in the Existing Smart City Infrastructure. *Journal of Organizational and End User Computing*, *32*(4), 85–111. doi:10.4018/JOEUC.2020100105

Habibi Lashkari, A., Draper Gil, G., Mamun, M. S. I., & Ghorbani, A. A. (2017). Characterization of Tor Traffic using Time based Features. *Proceedings of the 3rd International Conference on Information Systems Security and Privacy,* 253–262. doi:10.5220/0006105602530262

Hamidi, H., & Jahanshahifard, M. (2018). The Role of the Internet of Things in the Improvement and Expansion of Business. *Journal of Organizational and End User Computing*, *30*(3), 24–44. doi:10.4018/JOEUC.2018070102

Hamza, A., Gharakheili, H. H., & Sivaraman, V. (2018). Combining MUD Policies with SDN for IoT Intrusion Detection. *Proceedings of the 2018 Workshop on IoT Security and Privacy - IoT S&P '18*, 1–7. doi:10.1145/3229565.3229571

Hamza, A., Ranathunga, D., Gharakheili, H. H., Roughan, M., & Sivaraman, V. (2018). Clear as MUD: Generating, Validating and Applying IoT Behaviorial Profiles. *Proceedings of the 2018 Workshop on IoT Security and Privacy - IoT S&P '18*, 8–14. doi:10.1145/3229565.3229566

Hayashi, N. (2017). Connectivity Technologies_Nptel. Infectious Disease Magazine, 91.

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Networks*, *20*(8), 2481–2501. doi:10.1007/s11276-014-0761-7

Karimi, A. M., Niyaz, Q., Sun, W., Javaid, A. Y., & Devabhaktuni, V. K. (2016). Distributed network traffic feature extraction for a real-time IDS. *2016 IEEE International Conference on Electro Information Technology (EIT),* 522–526. doi:10.1109/EIT.2016.7535295

Laner, M., Svoboda, P., Nikaein, N., & Rupp, M. (2013). Traffic models for machine type communications. *10th IEEE International Symposium on Wireless Communication Systems 2013, ISWCS 2013, 9*, 651–655.

Lin, H., & Bergmann, N. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *Information (Basel)*, *7*(3), 44. doi:10.3390/info7030044

Lobaccaro, G., Carlucci, S., & Löfström, E. (2016). A review of systems and technologies for smart homes and smart grids. *Energies*, *9*(5), 1–33. doi:10.3390/en9050348

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Breitenbacher, D., Shabtai, A., & Elovici, Y. (2018). N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders. *IEEE Pervasive Computing*, *13*(9), 1–8. doi:10.1109/MPRV.2018.03367731

Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N. O., Guarnizo, J. D., & Elovici, Y. (2017, September). *Detection of Unauthorized IoT Devices Using Machine Learning Techniques*. https://arxiv.org/abs/1709.04647

Pishva, D. (2017). Internet of Things: Security and privacy issues and possible solution. *International Conference on Advanced Communication Technology, ICACT*. doi:10.23919/ICACT.2017.7890229

Polk, T., & Turner, S. (2014). Security Challenges For the Internet Of Things. *Workshop on Interconnecting Smart Objects with the …*, 638–643. doi:10.1109/MIPRO.2016.7522219

Romano, F. L., Ambrosano, G. M. B., Magnani, M. B. B. de A., & Nouer, D. F. (2005). Analysis of the coefficient of variation in shear and tensile bond strength tests. *Journal of Applied Oral Science*, *13*(3), 243–246. doi:10.1590/S1678-77572005000300008 PMID:20878024

Salman, O., Elhajj, I. H., Chehab, A., & Kayssi, A. (2019, May). A machine learning based framework for IoT device identification and abnormal traffic detection. *Transactions on Emerging Telecommunications Technologies*, 1–15. doi:10.1002/ett.3743

Sanatinia, A., Narain, S., & Noubir, G. (2013). Wireless spreading of WiFi APs infections using WPS flaws: An epidemiological and experimental study. *2013 IEEE Conference on Communications and Network Security, CNS 2013*, 430–437. doi:10.1109/CNS.2013.6682757

Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, *2017*, 1–25. Advance online publication. doi:10.1155/2017/9324035

Sivanathan, A., Gharakheili, H. H., Loi, F., Radford, A., Wijenayake, C., Vishwanath, A., & Sivaraman, V. (2019). Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics. *IEEE Transactions on Mobile Computing*, *18*(8), 1745–1759. doi:10.1109/TMC.2018.2866249

Sivanathan, A., Sherratt, D., Gharakheili, H. H., Radford, A., Wijenayake, C., Vishwanath, A., & Sivaraman, V. (2017). Characterizing and classifying IoT traffic in smart cities and campuses. *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 559–564. doi:10.1109/INFCOMW.2017.8116438

Statista. (2018a). *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)*. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Statista. (2018b). *The Internet of Things (IoT)* units installed base by category from 2014 to 2020 (in billions)*. https://www.statista.com/statistics/370350/internet-of-things-installed-base-by-category/

Stergiou, C., Psannis, K. E., Gupta, B. B., & Ishibashi, Y. (2018). Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT. *Sustainable Computing: Informatics and Systems*, *19*, 174–184. doi:10.1016/j.suscom.2018.06.003

Vaz, M. A. B., Pacheco, P. S., Seidel, E. J., & Ansuj, A. P. (2017). Classification of the coefficient of variation to variables in beef cattle experiments. *Ciência Rural*, *47*(11), 9–12. doi:10.1590/0103-8478cr20160946

Yang, H., Lee, W., & Lee, H. (2018). IoT Smart Home Adoption: The Importance of Proper Level Automation. *Journal of Sensors*, *2018*, 1–11. doi:10.1155/2018/6464036

Ivan Cvitić is born on December 18, 1986, in Zagreb. At the Faculty of Transport and Traffic Sciences, University of Zagreb, he finished undergraduate (2011) and graduate (2013) study of transport, information and communications traffic field. In 2014 started working as a teaching assistant at the Department of Information and Communication Traffic, Faculty of Transport and Traffic Sciences, University of Zagreb. In the same year he enrolled in postgraduate doctoral studies at the same institution. He received his PhD (summa cum laude) in 2020 by defending his PhD thesis titled Network traffic anomaly detection based on traffic characteristics and device class affiliation. He is actively engaged in scientific and research work in the field of information and communication traffic focusing on security research and the availability of information and communication services. Along with the above mentioned, he is actively researching the possibility of using the network forensics analysis of information and communication system. He is conducting research as an associate in the Laboratory for Security and Forensic Analysis of Information and Communication System. As a result of research activities, he published 43 scientific papers in scientific journals indexed in CC (Current Content), SCI (Social Citation Index), SCI-E (Social Citation Index - Expanded) and Scopus bases, and proceedings of international scientific conferences and scientific books. As an associate he was and still is involved in several projects funded by University of Zagreb, Faculty of Transport and Traffic Sciences and the Ministry of the Interior: System of Automated Identification and Information of Mobile Entities in the Traffic System (2015-2016), Impact of Using Mobile Devices on Driver Behavior While Driving (2017-2018), Analysis of Data Traffic Characteristics Generated by Various Terminal Devices (2017-2020), European Cooperation in Science and Technology (COST) - Digital Forensics Evidence Analysis via Intelligent Systems and Practices (DigForAsp) (2018 – ongoing). He has received several awards and recognitions. In 2013 he was awarded the Dean's award for student work entitled Development of queue management system of Faculty of Transport and Traffic Sciences student service. In 2015, based on the quality of the scientific paper entitled Classification of Security Risks in IoT Environment, he was awarded the FESTO Scholarship for the purpose of attending the 4th International Danube Adria Association for Automation and Manufacturing (DAAAM). That same year he received the award of the International Scientific Conference DAAAM 2015 for the best presentation of the aforementioned paper.

Dragan Peraković received B.S degree at the University of Zagreb, Faculty of Transport and Traffic Sciences (FTTS) 1995th, 2003. defended masters and 2005. Ph.D. dissertation named: A model of distribution of information to users of the transport system, at the FTTS. Dragan is Head of the Department for Information and Communication Traffic and Head of Chair of Information Communication Systems and Services Management, all at the FTTS where he is currently a full professor. Area of scientific interests and activities is modelling of information and communication systems and their applications in the environment of the transport system and Industry 4.0, simulation, e-forensic of information and communication systems / terminal devices / services, design and development of new innovative services and modules, e-Learning, ICT as assistive technologies for inclusion of people with disabilities. Dragan is author/co-author 4 CC indexed paper and more than 130 scientific papers in journals and proceedings of international conferences and 12 chapters in international scientific books. He participated in the work of several scientific projects and research & development studies. He is a member of TM Forum, IEEE, DAAAM International, SDIWC, EAI - European Alliance for Inovation, Association for promotion of innovative technologies InnovativeFET. Dragan is first chief editor of the International Journal of Cyber-Security and Digital Forensics (IJCSDF). Dragan is MC member in COST action CA17124 - Digital forensics: evidence analysis via intelligent systems and practices (DigForAsp).

Marko Periša is an Assistant Professor, Head of Chair of Information Communication Systems and Networks Head of the Laboratory of Development and Research of Information and Communication Assistive Technology Fields of interest: The development and the application of assistive technologies for people with disabilities in the traffic environment The development of e-business The development of information and communication technologies and services in order to enhance the quality of life of persons with disabilities Research in the field of Industry 4.0 / 5.0 and Society 5.0 concept development.

Mirjana D. Stojanović received the B.Sc. and M.Sc. degrees in electrical engineering and the Ph.D. degree in technical sciences from the University of Belgrade, Serbia, in 1985, 1993, 2005, respectively. She held research position with the Mihailo Pupin Institute, University of Belgrade, and was involved in developing telecommunication equipment and systems for regional power utilities and major Serbian corporate systems. She is currently a Full Professor of information and communication technologies with the Faculty of Transport and Traffic Engineering, University of Belgrade. She has participated in a number of National and International Research and Development Projects. As an author or coauthor she published more than 170 book chapters, journal articles, and conference papers in her field (56 citations and h-index 4, according to Scopus). She was the Lead Editor of the book on ICS cyber security in the Future Internet environment. She also published a monograph on teletraffic engineering and two university text-books (in Serbian). Her research interests include communication protocols, cyber security, service and network management, and the future internet technologies.